Towards quantum distance bounding protocols

Aysajan Abidin, Eduard Marin, Dave Singelée, and Bart Preneel

ESAT-COSIC and iMinds KU Leuven
Kasteelpark Arenberg 10, box 2452
3001 Heverlee, Belgium
firstname.lastname@esat.kuleuven.be

Abstract. Distance Bounding (DB) is a security technique through which it is possible to determine an upper-bound on the physical distance between two parties (denoted as verifier and prover). These protocols typically combine physical properties of the communication channel with cryptographic challenge-response schemes. A key challenge to design secure DB protocols is to keep the time required by the prover to process the challenges and compute and transmit the responses as low as possible. For this purpose, different implementation approaches have been proposed in the literature, both in the analog as in the digital domain. Moreover, different types of communication channels have been proposed as well to find an optimal balance between security and implementation feasibility. This paper is the first to evaluate the feasibility of implementing DB protocols using quantum communication. Unlike conventional DB protocols, which execute the rapid-bit exchanges over a Radio Frequency (RF) or ultrasound channel, our quantum-based DB protocol makes use of quantum-bit (qubit) transmissions and detection during the challenge-response phase. Our protocol offers security against distance fraud, mafia fraud and terrorist attacks. We also discuss how to protect against some specific implementation attacks, such as double read-out and quantum attacks, and give an overview of the main implementation challenges as well as possible limitations.

Key words: Distance bounding, Quantum transmission and measurement, Qubits.

1 Introduction

Distance Bounding (DB) protocols allow to establish an upper-bound on the physical distance between two parties which are typically denoted as verifier and prover. For this, DB protocols rely on cryptography and physics. For example, RF-based DB protocols leverage on the fact that it is impossible for adversaries to transmit signals faster than the speed of light. Brands and Chaum [1] were the first to introduce a DB protocol to counter relay attacks in Automatic Teller Machines (ATM) systems. Subsequently, a number of articles [2,3,4,5,6,7,8] has contributed not only to improve or

design new DB protocols, but also to implement these protocols. There are two main families of DB protocols: those that are derived from the protocol proposed by Brands and Chaum [1] and the ones that are based on the protocol proposed by Hancke and Kuhn [2]. All DB protocols have a *setup* and a *rapid-bit exchange phase*. In the setup phase, the verifier and the prover agree or commit to some information that will be used in the next protocol phase(s). In the rapid-bit exchange phase, which is the most difficult phase to implement due to severe timing constraints, the verifier sends a series of single-bit challenges to which the prover replies with single-bit responses. The verifier can then obtain its distance to the prover by measuring the Round-Trip Time (RTT) between sending its challenge and receiving the response from the prover. In some DB protocols, there is also a *verification phase* for checking that all protocol steps were performed using the parameters previously agreed on.

The goal of DB protocols is typically to protect against the following attacks: (i) *distance fraud*, (ii) *mafia fraud* and (iii) *terrorist fraud*. In a distance fraud attack, a dishonest prover tries to convince a verifier that it is in the verifier's close proximity while in reality it is far away. Mafia fraud (or relay attacks) involve an honest prover, a verifier and a Man-In-The-Middle (MITM) adversary. More specifically, the adversary uses a proxy-prover close to the verifier and a proxy-verifier close to the legitimate prover to relay over a long distance the messages exchanged between both parties. In a terrorist fraud attack, a dishonest prover collaborates with the adversary to convince the verifier that he is in its close proximity, while actually it is the adversary who is close to the verifier. It is common to assume that the prover only wants to collude with the adversary without revealing any information about its long-term secret key. This would prevent any attempt by the adversary to use the long-term secret key to conduct attacks at a later stage.

Our contributions. This paper investigates the feasibility of implementing quantum-based distance bounding protocols. The main physical principle upon which our protocol is based, is that unlike bits sent over conventional channels, qubits cannot neither be measured without modifying their states nor be decoded before fully receiving them. Without knowing the basis of the qubits, which the prover and verifier agreed upon based on a shared secret key, adversaries can only guess the qubits that are being sent. Therefore, our proposal by itself is resistant to some of the well-known DB attacks. We also note that our proposal could be transformed into a post-quantum DB by just replacing the PseudoRandom Function (PRF), used in the initialisation phase, by a post-quantum

PRF. Based on a theoretical analysis, we estimate the delay introduced by each of the hardware components at the prover, and conclude that our solution keeps this delay at a reasonable level compared to other implementation approaches. Finally, we also evaluate our scheme against some implementation-specific attacks, more in particular double read-out and quantum attacks, and then elaborate on the main implementation challenges and possible limitations.

Paper outline. Section 2 gives an overview of related work. Section 3 provides the necessary background on quantum communication and qubits. Next, section 4 describes our quantum-based distance bounding protocol, whereas a detailed security analysis of our solution is given in Section 5. Section 6 discusses the feasibility of our proposed implementation approach. Section 7 gives concluding remarks.

2 Related work

The security provided by DB protocols, which measure the RTT to estimate the distance between prover and verifier, relies on the fact that the prover is able to process the challenge and then compute and transmit the response in negligible time compared to the propagation time. If the verifier overestimates the prover's processing time (i.e., the prover can process the challenge faster), the prover can pretend to be closer than it actually is. On the contrary, if the verifier underestimates the prover's processing time, the prover may not be able to successfully execute the DB protocol with the verifier, even when it is in its close proximity. As the processing time depends only on the prover's hardware, which is not under the control of the verifier, for DB protocols to be resistant to attacks the processing time at the prover needs to be as close as possible to zero.

Intuitively, one possibility would be to send the response over an ultrasonic channel, provided that this channel is relatively slow compared to the processing time at the prover. However, ultrasonic-based DB protocols are vulnerable to worm-hole attacks [9]. This attack involves a MITM adversary who uses both a proxy-prover and a proxy-verifier to convert the audio signal to a radiofrequency (RF) signal (and vice versa) in order to accelerate the transmission time on the relay channel. This would allow adversaries to extend the maximum distance from which the verifier successfully authenticates the prover by several orders of magnitude.

For practical realisations of DB protocols over an RF channel, the main challenge for the prover is to compute the response using a function that can be executed significantly fast. We distinguish between two types

of functions, depending on whether they are conducted in the analog or digital domain. Brands and Chaum [1] proposed that the response sent by the prover is the result of the XOR between the challenge and a value agreed upon between the verifier and the prover in the setup phase. Hancke and Kuhn [2] proposed to choose a value from two locally stored registers at the prover depending on the challenge sent by the verifier. Although both operations are relatively simple, they require the prover to convert the signal from the analog to the digital domain using an Analog-to-Digital Converter (ADC), demodulate the signal to obtain the challenge bit, compute and modulate the response bit and convert the signal from the digital to the analog domain using a Digital-to-Analog Converter (DAC). This process typically results in a processing time delay in the order of at least a few hundred nano seconds. This large delay allows adversaries with dedicated hardware to successfully execute the protocol with the verifier from several dozen meters away.

Another approach consists of computing the response by the prover based on a function that can be directly executed in the analog domain. Rasmussen and Capkun proposed an analog function – which they call Challenge Reflection with Channel Selection (CRCS) – for which the prover reflects the challenges sent by the verifier in a specific way depending on the received challenge and the response (i.e. the value of the register) [4]. The prover demodulates the signal to recover the challenges only after finishing the rapid-bit exchange phase. This approach does not introduce any delay in the time-critical rapid-bit exchange phase, while still allows the prover to prove knowledge of the challenge bits in the last protocol phase. However, Ranganathan et al. found that the CRCS implementation is vulnerable to a double read-out attack, which allows an adversary to obtain the values of the prover's two registers simultaneously [6]. Ranganathan et al. proposed an hybrid solution – which they call Switched Challenge Reflector with Carrier Shifting (SCRCS) – that prevents the double read-out attack by introducing a new digital component that disables part of the analog circuitry after detecting the challenge [6]. However, both the analog and hybrid approaches require complex hardware and storage at the prover.

We are the first to investigate the feasibility of implementing DB protocols using quantum communication. The closest work to ours is the quantum-based positioning system proposed by Buhrman et al. [10]. In their paper, multiple verifiers interact with the prover to determine its position. In our paper, we apply quantum techniques to DB protocols.

3 Background on quantum communication

In the classical (non-quantum) domain, communication can always be eavesdropped or copied. This is in contrast to quantum communication where the transmitted information is encoded in non-orthogonal quantum states that cannot be reliably read or copied, due to the Heisenberg uncertainty principle in quantum physics. Any attempt by an adversary to eavesdrop the quantum communication will introduce random errors.

Qubits. A qubit is a unit of quantum information, just as a bit (0 or 1) is the classical unit of information. A qubit is a vector in a 2-dimensional Hilbert space (a vector space with inner product). The basis $\{|0\rangle = \begin{bmatrix}1\\0\end{bmatrix},\ |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}\}$ for a qubit is called the computational basis, while the basis $\{|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2},\ |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$ is called the diagonal (or the Hadamard) basis. In general, a normalised quantum state can be expressed as a superposition of $|0\rangle$ and $|1\rangle$ as

$$a\,|0\rangle + b\,|1\rangle\,,$$

where $a, b \in \mathbb{C}$ satisfying $|a|^2 + |b|^2 = 1$.

If we measure a qubit in state $a\,|0\rangle + b\,|1\rangle$ in the computational basis (i.e., if the state is projected on the computational basis), then with probability $|a|^2$ we obtain $|0\rangle$ and with probability $|b|^2$ we obtain $|1\rangle$. If the state of a qubit is unknown, the values a and b cannot be determined with a single measurement. And after a measurement, say in the $\{|0\rangle\,,\ |1\rangle\}$ basis, the qubit state collapses into $|0\rangle$ or $|1\rangle$, which is different from the original state.

Now let us take a closer look at the four states: $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$. It is straightforward to see that:

$$|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$$

and

$$|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}.$$

Therefore, if the qubits $|0\rangle$ and $|1\rangle$ are measured in the computational basis (i.e., projected onto the $\{|0\rangle\,,\ |1\rangle\}$ basis), then the states are not disturbed; whereas the measurement in the Hadamard basis destroys the state, since in this case $|+\rangle$ and $|-\rangle$ are obtained with equal probability. Similarly, if the qubits $|+\rangle$ and $|-\rangle$ are measured in the Hadamard basis, then the states are not disturbed; whereas the measurement in the computational basis

destroys the state, since in this case $|0\rangle$ and $|1\rangle$ are obtained with equal probability. It is exactly this principle that we will use in our protocol.

More specifically, in our proposal we make use of these four states, which are usually called the BB84 states in quantum key distribution (QKD) [11]. Namely, we propose to implement the rapid challenge-response phase of a DB protocol by employing qubits, as opposed to the classical approach using RF signals or ultra-wide-band (UWB) pulses. These four states correspond to different polarisations of photons. These photons are sent from prover to verifier, or vice versa, via laser beams. The states $|0\rangle$ and $|1\rangle$ respectively correspond to horizontally $\rightarrow$ and vertically $\uparrow$ polarised photons, while the states $|+\rangle$ and $|-\rangle$ to $\nearrow$ and $\nwarrow$ polarised photons. The qubit $|0\rangle$ or $|+\rangle$ is used to encode the classical bit value 0 and $|1\rangle$ or $|-\rangle$ the value 1. The qubits are measured either in the computational or the Hadamard basis. In what follows, we let 0 to denote the computational $(+)$ basis and 1 the Hadamard $(\times)$ basis.

Table 1: An encoding rule. In our proposal, the value 0 corresponds to the computational (or simply + basis), and 1 to the Hadamard (or simply $\times$) basis.

Data	Computational (or +) basis	Hadamard (or $\times$) basis
0	$\|0\rangle$ (i.e., $\rightarrow$)	$\|+\rangle$ (i.e., $\nearrow$)
1	$\|1\rangle$ (i.e., $\uparrow$)	$\|-\rangle$ (i.e., $\nwarrow$)

4 Our quantum-based distance bounding protocol

Our approach is based on the exchange of polarised photons. Similarly as in the DB protocol of Hancke and Kuhn, the prover and verifier first execute a setup phase in which random nonces are exchanged. Based on these nonces and a shared secret, both parties compute the output a of a PseudoRandom Function (PRF). During the rapid-bit exchange phase, the verifier encodes randomly chosen challenge bits into polarisation states of photons in the bases determined by the bitstring a.

For example, if $a_i = 0$, then a challenge bit 0 would be encoded as the $\rightarrow$ photon, whereas a challenge bit 1 would be encoded as the $\uparrow$ photon. Similarly, if $a_i = 1$, then a challenge bit 0 would be encoded as the $\nearrow$ polarised photon, whereas a challenge bit 1 would be encoded as the $\nwarrow$ polarised photon. If $a = 01011$ and the challenge bits are 10010, then a series of photons polarised as $\uparrow$, $\nearrow$, $\rightarrow$, $\nwarrow$, $\nearrow$, respectively, will be sent by

the verifier. The prover then decodes the photons in the bases determined by the PRF output (denoted as a) and sends its responses as photons that encode the decoded results in the bases determined by the bits of a. Since the encoding and decoding bases are the same, the verifier receives photons in the same polarisation states as the ones that were sent. From the RTT of the photons, the verifier calculates an upper-bound on the physical distance between itself and the prover.

This is similar to QKD, except that now the two communicating parties use the same bases as opposed to the randomly chosen bases in the case of QKD. An adversary would need to guess what encoding basis is used to successfully intercept and decode the verifier's signal and then send the result back to the verifier. Therefore, there is a 50% chance that the adversary guesses wrong. Thus, as a consequence of the quantum *uncertainty principle*, the adversary will destroy the information encoded by the verifier and render the received responses uncorrelated to the challenges that are sent.

A schematic description of a DB protocol employing the aforementioned technique, using polarised photons, is given in Fig 1. As can be seen, during the challenge-response phase, instead of sending and receiving classical challenge-response pairs, the verifier sends and receives quantum challenge-response pairs. As long as the prover is the legitimate prover with whom the verifier computed $a = f_{x_p}(N_v, N_p)$, the verifier always receives photons that are in the same polarisation states as the ones that are sent, since the photons are encoded/decoded in the same bases determined by the bit values of a. The prover stores the decoded bits in a register c and uses them during the verification phase. In this third phase of the protocol, the prover computes a MAC on the ID of prover and verifier, the nonces exchanged in the setup phase, and the bitstring c. This last step is critical for security. Without the prover sending a MAC in the verification phase, an adversary could just reflect all the photons back to the verifier without actually performing any measurements at all.

To summarise, the main components needed for our solution are an encoder, a decoder, and a data processing unit. The encoder consists of a tuneable polariser which polarises incoming photons or laser pulses. The incoming pulses are polarised according to the previously mentioned encoding rule, e.g., $c = 0$ is encoded as $\nwarrow$ polarised photon if the corresponding register value is 1. The decoder consists of a detector and a data processing unit. The detector measures the photons in $+$ basis if the register value is 0 and in $\times$ basis if the register value is 1. The data processing unit analyses the measurement result and outputs 0/1.

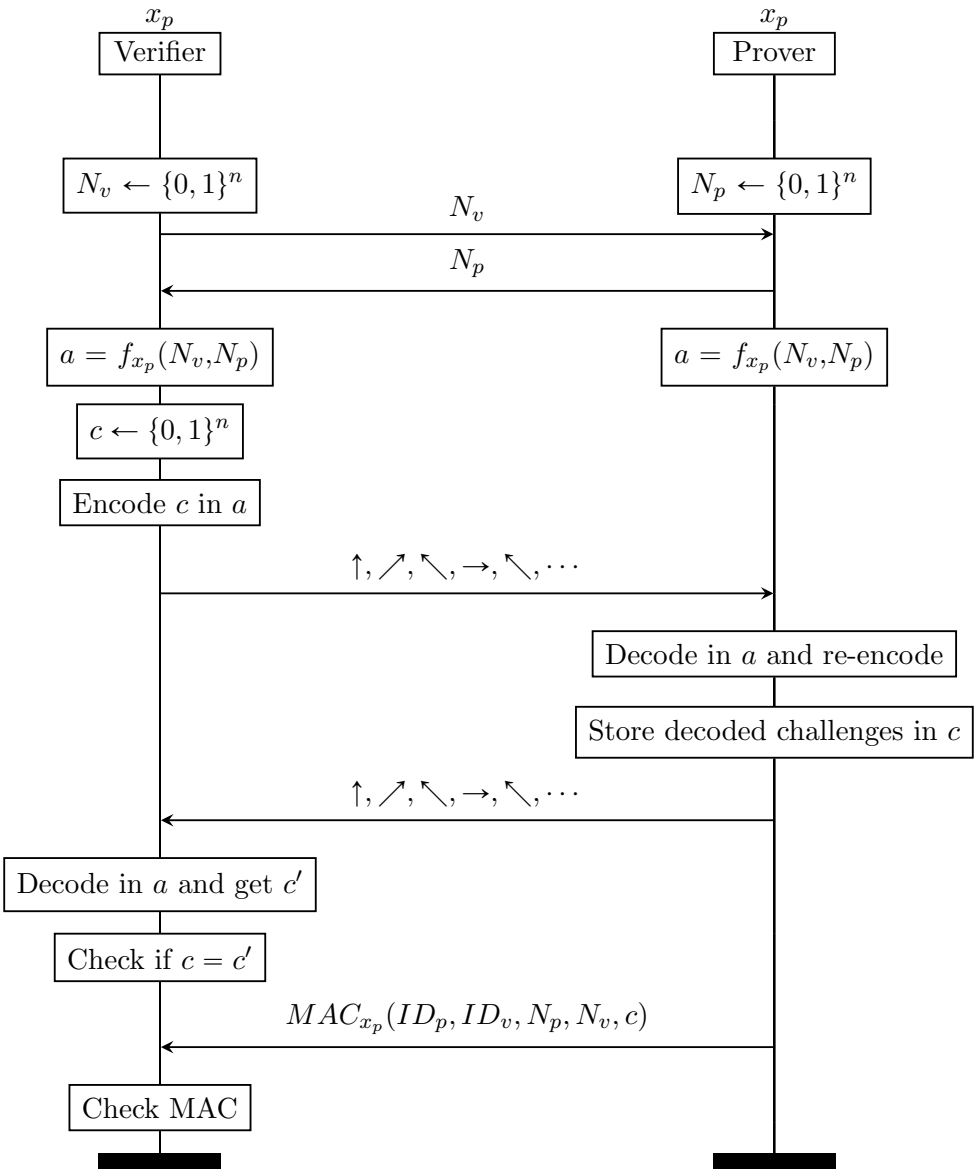

Fig. 1: Example of a quanutm-based DB protocol using polarised photons in the rapid-bit exchange phase. It should be noted that each challenge is sent only after the verifier received the response to the previous challenge.

5 Security Analysis

This section analyses the resistance of our protocol to distance fraud, mafia fraud and terrorist fraud attacks. In addition, we identify two implementation-specific attacks, and show how to prevent them. We also present some of the possible limitations when realising quantum-based DB protocols.

5.1 Protocol Analysis

Distance fraud attack. A dishonest prover can attempt to shorten the distance to the verifier in several ways. The adversary can either (i) predict the challenge, (ii) reply before fully receiving the challenge (i.e. lower the processing delay by replying too early) or (iii) try to reduce the processing delay by using more sophisticated hardware components. However, as the verifier chooses its challenges at random, if the adversary opts for sending its response before receiving the challenge, he can guess the challenges sent by the verifier only with probability $(1/2)^n$. Furthermore, due to the properties of qubits, it is impossible for adversaries to learn their value before fully receiving them. This is in contrast with conventional RF-based systems, where one can learn the value of a bit by only partially decoding the received signal [12].

The existing distance bounding implementations provide processing time delays at the prover in the order of 1-100 ns. Fig 2 shows the hardware components used by the verifier and the prover in our proposal. We estimate that the processing delay at the prover will be approximately 10 ns, as this is typically the usual delay in practical QKD implementations. Thus, an adversary can (at best) shorten the distance by 3 meters. While our proposal introduces a processing time delay that is slightly higher than some of the analog and hybrid solutions, it decreases the hardware complexity of the system.

Mafia fraud attack. Adversaries can follow two different strategies to perform mafia fraud attacks: (i) *early-detect and late-commit* or (ii) *replay-and-forward*.

The *early-detect and late-commit attack* can be divided into four steps: (i) early-detect the challenge from the verifier, (ii) forward the challenge to the prover, (iii) early-detect the response from the prover and (iv) forward the response to the verifier. However, our solution by itself is resistant to this attack, since it is impossible for adversaries who do not know the correct basis to measure the photons without modifying their states.

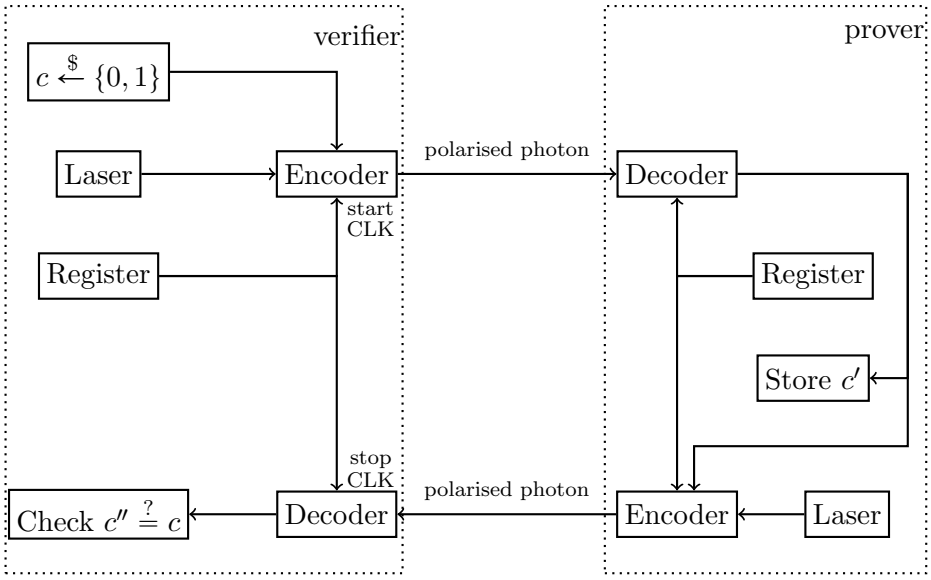

Fig. 2: High-level schematic description of our quantum-based approach during one challenge-response round. The verifier selects a random challenge bit c, encodes it into a polarisation of a photon emitted from the photon source (Laser) in the basis determined by the first bit of the Register, and starts the clock. The prover decodes the photon in the basis determined by the first bit of the Register and obtains c', which is then encoded into a polarisation of a photon emitted from the prover's photon source (Laser) in the same basis used for decoding. The prover also stores c', which will be used later in the verification phase. The verifier decodes the incoming photon in the basis previously used to encode the challenge bit and obtains c'', stops the clock, and checks whether $c'' = c$. This process is repeated as many times as the number of bits in the Register. If the number of rounds in which $c'' = c$ is above a threshold, then the verifier can use the maximum of all the RTT to compute the physical distance of the prover.

In the *replay-and-forward attack*, the adversary reflects the challenge to the verifier while still being able to forward the challenge to the prover. To perform this attack, the adversary would have to use a Photon Number Splitter (PNS). It is important to point out that this attack, which is analogous to PNS attacks on QKD implementations, can only be conducted if the challenge contains more than one photon per pulse. In that case,

the adversary could reflect one photon, and decode another photon in the same pulse. The goal of the adversary is to convince the verifer that the prover decoded and encoded the photon correctly. Since our protocol has a verification phase where the prover proves knowledge of the challenges sent by the verifier, the adversary needs to forward the challenge to the prover as well. To prevent this attack, one has to avoid that photons in a pulse can be splitted. Therefore, it is necessary to use efficient single-photon sources in the design, and hence select the most appropriate laser source.

Assuming the photon splitting attack is prevented by the selection of the laser source, the mafia fraud attack succeeds with probability $\left(\frac{3}{4}\right)^n$, *i.e.* an adversary can pre-ask the prover for responses – if he guesses the pre-asked challenge correctly he always wins the round, otherwise he needs to guess the response with probability $\left(\frac{1}{2}\right)$.

Terrorist fraud attack. In the literature, protocols that are terrorist-fraud resistant are all based on a similar design approach [13]. Therefore to make our protocol terrorist-fraud resistant, one needs to implement a response function where the prover's key is revealed if the prover discloses all the possible responses (i.e. the outputs of the PRF) to the adversary. To achieve this, the register (a in our protocol) is constructed as follows. The first half of the register is the output of the PRF, while the second half is the XOR of the first half with the shared long-term key. This way, the adversary would learn the prover's secret long-term key if the register a would be shared with him. As a result, the prover can share only half of the registers with the adversary, meaning that the adversary knows half of the responses and needs to guess the rest. The success probability for terrorist fraud is therefore $\left(\frac{3}{4}\right)^n$.

5.2 Implementation attacks

No-photon attack. Most lasers typically emit a small number of photons per pulse (e.g. 0.3 photons per pulse) that are distributed according to a Poisson distribution. As a result, most pulses have no photons, some others contain 1 photon, and only a few contain 2 or more photons. We can distinguish between three types of situations for each of the protocol rounds: (i) when a single photon is sent per pulse, (ii) when two (or more) photons are sent per pulse and (iii) when no photon is sent per pulse. The first case will not be studied further since it is the ideal case and does not introduce any security problems. The second case is relevant to perform mafia fraud attacks and is explained above. In the third case, the adversary does not need to send any response at all. This would drastically reduce the security level of the protocol, since the adversary wins in all

rounds where no pulses are being sent. To overcome this limitation, one could increase the number of rounds of the protocol, to ensure that there are sufficient rounds with at least one photon being exchanged.

Double read-out attack. The goal of this attack is to exploit the specific implementation of the DB protocol to obtain the values of the two registers of the prover. A similar attack could be performed on our scheme to obtain the bases being used by the prover and the verifier. The adversary could recover the basis being used only if the prover would reuse a basis to measure different challenges and responds to each of these challenges. In practice, the attack would work as follows: the adversary first lets the prover and the verifier start executing the protocol and exchanging the nonces. The adversary then follows a pre-ask strategy, it first executes the rapid-bit exchange phase with the prover to obtain the basis being used and then executes the protocol with the verifier. For this, the adversary first encodes a photon using a basis (chosen at random) and sends it to the prover. The idea is that the adversary exploits the implementation of the protocol by sending multiple photons, using the same base, during one round of the protocol. We can distinguish between two situations depending on whether the adversary has guessed the basis used by the prover. If so, then all the challenges (i.e. photons) sent during the same round will be decoded correctly by the prover, and all the responses will be equal to the challenges. If the guess was wrong, the prover encodes the bits using the wrong basis, and will obtain random bits for each of these challenges. The adversary will notice that the responses are not equal, and hence the wrong basis was used.

The key aspect of this attack is that the adversary could send multiple challenges during a single round. To prevent this type of attack, the prover needs to have a reliable detector that updates its setting after measuring the challenges (i.e. switch to the basis of the next round) and hence avoids basis reuse in a single round.

6 Feasibility analysis

Our proposal is similar to the quantum transmission and measurement phase of a BB84 type QKD protocol. The only difference is that in our case the preparation and measurement bases for the qubits are kept secret, while they are publicly announced in QKD. QKD has long been successfully implemented, and there are even commercially available QKD products. Since the QKD setup for the quantum transmission and measurement can be used as is to experimentally realise our proposal, the feasibility of

our proposal is not an issue. However, we are interested in keeping the actual processing delay at the prover as low as possible. While the actual experimental demonstration is beyond the scope of this paper, based on the experimental results on QKD we estimate that the delay can be around 10 ns. In future work, we want to perform experiments using the QKD setup to validate the short processing delay of our proposed solution.

The three main components on both the prover and verifier sides are a single photon source, a single photon detector, and a data processing unit. All of these components are available on the market.

7 Conclusions

This paper has investigated the feasibility of implementing distance bounding protocols based on quantum communication. We proposed a quantum-based distance bounding protocol that uses a function to compute the prover's response based only on knowing the basis to measure the quantum bits. We analysed its security against various attacks and gave a theoretical analysis of the processing delay at the prover.

Acknowledgments. The authors would like to thank the anonymous reviewers for their helpful comments. This work was partially supported by the Research Council KU Leuven: C16/15/058 and by the European Commission through the SECURITY programme under FP7-SEC-2013-1-607049 EKSISTENZ.

References

1. Brands, S., Chaum, D.: Distance-bounding protocols (extended abstract). In: EUROCRYPT. (1993) 344–359
2. Hancke, G.P., Kuhn, M.G.: An rfid distance bounding protocol. In: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks. SECURECOMM '05, Washington, DC, USA, IEEE Computer Society (2005) 67–73
3. Tippenhauer, N.O., Čapkun, S.: Id-based secure distance bounding and localization. In: Proceedings of the 14th European Conference on Research in Computer Security. ESORICS'09, Berlin, Heidelberg, Springer-Verlag (2009) 621–636
4. Rasmussen, K.B., Čapkun, S.: Realization of rf distance bounding. In: Proceedings of the 19th USENIX Conference on Security. USENIX Security'10, Berkeley, CA, USA, USENIX Association (2010) 25–25
5. Singelee, D., Preneel, B.: Distance bounding in noisy environments. In: European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS), Springer-Verlag LNCS 4572, pp 101-115. (2007)

6. Ranganathan, A., Tippenhauer, N.O., Škorić, B., Singelée, D., Čapkun, S. In: Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System. Springer Berlin Heidelberg, Berlin, Heidelberg (2012) 415–432
7. Rasmussen, K.B., Castelluccia, C., Heydt-Benjamin, T.S., Capkun, S.: Proximity-based access control for implantable medical devices. In: Proceedings of the 16th ACM Conference on Computer and Communications Security. CCS '09 (2009) 410–419
8. Ranganathan, A., Danev, B., Capkun, S.: Proximity verification for contactless access control and authentication systems. In: Proceedings of the 31st Annual Computer Security Applications Conference. ACSAC 2015, New York, NY, USA, ACM (2015) 271–280
9. Sedighpour, S., Capkun, S., Ganeriwal, S., Srivastava, M.: Implementation of attacks on ultrasonic ranging systems (nov 2005)
10. Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R., Schaffner, C.: Position-based quantum cryptography: Impossibility and constructions. SIAM Journal on Computing **43**(1) (2014) 150–178
11. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proc. of the IEEE Int. Conf. on Computers, Systems, and Signal Processing. 175–179, Bangalore, India, IEEE New York (1984)
12. Clulow, J., Hancke, G., Kuhn, M., Moore, T.: So near and yet so far: Distance-bounding attacks in wireless networks. In: Proceedings of the 3rd European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS '06). Volume LNCS 4357 of Lecture Notes in Computer Science., Springer-Verlag (2006) 83–97
13. Reid, J., Gonzalez Nieto, J.M., Tang, T., Senadji, B.: Detecting relay attacks with timing-based protocols. In: Proc. of ASIACCS. (2007)